REMARKS

Claims 1-24 are pending in this application.

Applicant would like to thank the Examiner for the courtesy extended during the telephone interview on May 11, 2006 regarding the present claimed invention.

Rejection of Claims 1-9, 11-15, 18, 20, 21, 23 and 24 under 35 USC 103(a)

Claims 1-9, 11-15, 18, 20, 21, 23 and 24 are rejected under 35 USC 103(a) as being unpatentable over Levergood (US Pat. No. 5,708,780) in view of Calamera et al. (U.S. Patent No. 6,463,533). These claims are deemed patentable for the reasons given below.

The present claimed invention provides a system and method employed by a first application for encoding URL link data for use in detecting unauthorized URL modification. An input processor receives an encryption key. A URL processor adaptively processes a URL link to a second application differently to an intra-application link to a web page provided by the first application by using the received encryption key to encrypt a URL link address portion of the URL link to the second application to produce a processed URL and by non-encryption of the intra-application link. A communication processor includes the processed URL in data representing a web page and communicates the web page representative data including the processed URL to a requesting application. Independent claims 1, 11, 18, 20, 21, 23 and 24 include similar limitations to those described above.

Levergood describes an internet server access control and monitoring system. When a user selects a link that is directed to an access-controlled file, the server subjects the request to a secondary server which determines whether the client has an authorization or valid account. Upon verification, the user is provided with a session identification, allowing the user to access the requested file as well as any other files within the present protection domain.

Calamera describes a system for allowing a computer network site to recognize an anonymous user without revealing the identity of the user. The system involves generating a user alias such that it is computationally difficult to determine the user's identify from the alias alone (Calamera abstract). Applicant respectfully submits that Calamera (with Levergood) neither discloses nor suggests "a URL

processor...encrypt[ing] a URL link address portion of said URL link" as recited in the present claimed invention. Calamera does NOT encrypt an address portion of a URL, but a URL (domain plus path) together with a user identification code and a random number (column 7, lines 31-36, 42-57). Calamera uses an irreversible one-way hash function and does not encrypt a URL address portion (column 7, line 57).

Applicant respectfully submits that arguments presented in the Amendments filed November 30, 2004 and May 25, 2005 and the Appeal Brief filed September 6, 2005 distinguishing the present claimed system from Levergood and Calamera are applicable and are hereby incorporated by reference.

Specifically, the system of the present invention, is unlike Levergood (with Calamera) in that the claimed system involves "adaptively processing a URL link to a second application differently to an intra-application link to a web page provided by said first application". This is done "by using said received encryption key to encrypt a URL link address portion of said URL link to said second application to produce a processed URL and by non-encryption of said intra-application link". These features address the security deficiencies of URL processing functions of electronic systems, such as those described in Levergood (and Calamera). As stated on page 11, lines 1-9 of the present specification, "Applications are vulnerable to the corruption of URL data and the context information conveyed within the URL data. The URL data conveyed from application 200 to application 230 includes context information comprising a session identifier and optionally a user or patient identifier. This URL data is potentially vulnerable to corruption to cause URL replay or redirection of an application to a substitute address or to gain access to application functions and parameters for unauthorized purposes. In order to protect against such corruption and to ensure that the entity being accessed is the one originally targeted, portions of the URL data conveyed between applications are advantageously encrypted."

The claimed system addresses the security problem that is present in prior art systems such as Levergood (and Calamera) by "adaptively processing a URL link to a second application differently to an intra-application link to a web page provided by said first application by using said received encryption key to encrypt a URL link address portion of said URL link to said second application to produce a processed URL and by non-encryption of said intra-application link" as recited in the present invention. Further, user selection of an embedded link to view patient laboratory test orders via browser command, for example, does not require incorporation of a session

identifier and other context information, as stated in the present specification on page 14, lines 34-36, "because the link to the test results page is an intra-application link there is no requirement for this particular embedded link to be processed in the manner previously described to incorporate the session identifier and other context information".

Applicant further respectfully submits that there is no reason or motivation to combine the system disclosed by Levergood with the system disclosed by Calamera. Specifically, as discussed in the Examiner's Interview on May 11, 2006 and acknowledged by the Examiner, Levergood and Calamera are incompatible systems and thus cannot be combined to produce an operable system. Calamera teaches against conveying information in URL data fields for subsequent decryption in direct conflict with the encryption system of Levergood. Calamera states that the user's identity is NOT revealed (see col. 3, lines 6 – 9) and teaches that the encryption key is only held by the alias server system and cannot be used by any other system for decryption. Furthermore, unlike the present claimed invention, Calamera has no notion of session.

However, even if the combination of Levergood and Calamera were able to produce an operative system, the result would be a system that uses an irreversible encryption mechanism to encrypt an entire URL and **NOT** "an address portion" as in the present claimed invention. Calamera (with Levergood) neither discloses nor suggests "adaptively processing a URL link to a second application differently to an intra-application link to a web page provided by said first application" as recited in the present claimed invention. The references also fail to show or suggest doing this "by using said received encryption key to encrypt a URL link address portion of said URL link to said second application to produce a processed URL and by non-encryption of said intra-application link" as received in the present claimed invention.

In view of the above remarks, it is respectfully submitted that there is no 35 USC 112 enabling disclosure in either Levergood et al. or Calamera et al., when taken alone or in combination, that makes the present invention as claimed in claims 1, 11, 18, 20, 21, 23 and 24 unpatentable. Applicant further respectfully submits that as claims 2-9 are dependent on claim 1 and claims 12-15 are dependent on claim 11, these claims are patentable for the same reasons as claims 1 and 11 respectively. Consequently, it is respectfully submitted that this rejection is satisfied and withdrawal of the Rejection of Claims 1-9, 11-15, 18, 20, 21, 23 and 24 under 35 USC 103(a) is respectfully requested.

Rejection of Claims 10, 16, 17, 19 and 22 under 35 U.S.C. 103(a)

Claims 10, 16, 17, 19 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Levergood (U.S. Pat. No. 5,708,780) in view of Calamera et al. (U.S. Patent No. 6,463,533) and further in view of Berman (U.S. Pat. No. 5,995,939).

Berman describes a system and method for making and fulfilling service requests between two or more remote sites over the Internet or a similar computer network. Berman describes an SMTP (not HTTP protocol) system employing HL7. Additionally, Berman states that "[a]t the present time, e-mail messages sent over the Internet **must** be in standard SMTP format" (see Berman, col. 5, lines 61-62). Furthermore, Berman provides no 35 USC 112 compliant enabling disclosure of a URL, as recited in claims 10, 16, 17, 19 and 22 of the present invention.

Claim 10 is dependent on claim 1 and is thus considered to be patentable for the reasons given in connection with claim 1. Claim 16 includes features similar to those recited in claim 1 and therefore, the Arguments presented above and in the previously filed Amendments and Appeal Brief are applicable. Specifically, Levergood, Calamera and/or Berman neither disclose nor suggest "a URL processor for adaptively generating URL fields including an encrypted URL address portion and encrypted patient specific information for incorporation together with a non-encrypted portion in a processed URL" as in the present claimed invention. Therefore, Applicant respectfully submits that claim 16 is considered to be patentable for the reasons given above in connection with claim 1.

Applicant further respectfully submits that these references, alone or in any combination, fail to show or suggest "adaptively processing a URL link to a second application differently to an intra-application link to a web page provided by said first application." The combined references also fail to show or suggest doing this "by using said received encryption key to encrypt a URL link address portion of said URL link to said second application to produce a processed URL and by non-encryption of said intra-application link." Furthermore, the combined references fail to show or suggest a "URL processor" that "adaptively generates URL fields including encrypted patient specific information for incorporation" in a "URL link" to a "second application."

With respect to Claim 22, Applicant respectfully submits that in addition to the reasons discussed above, Levergood alone or in combination with Calamera and Berman neither disclose nor suggest a "forming a URL to provide a formed URL link by encrypting a link address to a second application and incorporating said encrypted link address, session identification information and **encrypted patient specific information** in said formed URL link" as in the present claimed invention. The method claimed in claim 22 adaptively generates fields including encrypted patient specific information for incorporation in said URL link to said second application. The cited references alone or in combination with one another provide no 35 USC 112 compliant enabling disclosure of this claimed feature.

Applicant respectfully submits that, as discussed above and acknowledged by the Examiner, Calamera teaches against conveying information in URL data fields for subsequent decryption. Calamera states that the user's identity is NOT revealed (see col. 3, lines 6 – 9) and teaches that the encryption key is only held by the alias server system and cannot be used by any other for decryption. Furthermore, unlike the present claimed invention, Calamera has no notion of session. Therefore, the system disclosed by Calamera is incompatible with the system disclosed by Levergood and their combination would be inoperative. It is further respectfully submitted that there is no reason or motivation to combine Berman with either of Levergood and/or Calamera as Berman provides no 35 USC 112 compliant enabling disclosure of URL's, but instead describes an SMTP system and neither discloses nor suggest a URL as in the present claimed invention.

In view of the above remarks, it is respectfully submitted that there is no 35 USC 112 enabling disclosure in Levergood et al., Calamera et al. and Berman et al. when taken alone or in any combination, that makes the present invention as claimed in claims 1, 16 and 22 unpatentable. Applicant further respectfully submits that as claim 10 is dependent on claim 1 and claim 17 is dependent on claim 16 and claim 19 is dependent on claim 18 discussed above, these claims are patentable for the same reasons as claims 1, 16 and 18 respectively. Consequently, it is respectfully submitted that this rejection is satisfied and withdrawal of the Rejection of Claims 10, 16, 17, 19 and 22 under 35 USC 103(a) is respectfully requested.

A Supplemental Information Disclosure Statement was filed on January 19, 2006 identifying U.S. Patent No. 6,971,067; 6,941,313 and 6,993,556 for consideration. Applicant respectfully submits that these Patents neither disclose nor suggest the present invention as claimed in claims 1 – 24. Therefore, Applicant further respectfully submits that systems disclosed in these patents provide no 35 USC 112 compliant enabling disclosure that would make the present claimed invention unpatentable.

In view of the above remarks, Applicant submits that the Application is in condition for allowance, and favorable reconsideration is requested.

Respectfully submitted,

Date: June 7, 2006

Alexander J. Burke
Reg. No. 40,425

Alexander J. Burke
Intellectual Property Department
Siemens Corporation,
170 Wood Avenue South
Iselin, N.J. 08830
Tel. 732 321 3023
Fax 732 321 3030